User ID:

Password: *********

Login

Úskalia autentifikácie

Ľubor Illek, Gordias sro., 2013

Autentifikácia

- Stále najčastejšie meno/heslo
- Funkčne triviálna
- Pre bezpečnosť kľúčová

- Veľa chýb – návrh, algoritmy, implementácia
- Veľké úniky údajov

⇨ Najčastejšia cesta kompromitácie

Heslá - stav

- priemerný používateľ: 26 účtov, 5 rôznych hesiel
- 40% zdieľa heslo s inými
- >98% účtov má heslo spomedzi 10.000 najčastejších
- 0,5% hesiel má špeciálny znak, 41% iba písmená
- úniky hesiel
  - Twitter - 250.000, LinkedIn – 6.500.000 (zverejnené)
  - Yahoo - 450.000 , NVidia, Last.fm...
  - eHarmony - 1,5M; 80% prelomených do 3 dní

Ukladanie hesla

- Štandardne v DB uložené meno používateľa a heslo?
- Postupný vývoj odporúčaní
  - ako rastie výpočtová kapacita
  - dnes štandardná technika, ustálený stav
  - viaceré „úrovne“ ochrany
- Základ: 1) jednocestná informácia - hash
  - redukovanie útokov na skúšanie/hrubú silu
  - nestačí - slovníky

2) Solenie

- Rovnaké heslo = rovnaký hash
  - ľahká detekcia zhody
  - Rainbow Tables - predpočítanie hashov
  - online služby na prelomenie
- Riešenie: pridať ďalší reťazec - salt
  - v DB uložené Hash(password + salt) aj salt
  - unikátny reťazec pre každú položku
  - dĺžka aspoň 64 bitov

3) Zosilnená funkcia

- Aký hash použit?
- Aktuálny útok hrubou silou
  - cca. 10^11 operácií za sekundu
  - za hodinu: všetky možnosti do dĺžky 8 zn. a-z,A-Z,0-9

- MD5 – prelomený, SHA – nedostatočné
- NTLM – prelomené...

3) Zosilnená funkcia

- Špecializované funkcie:
  - PBKDF2 (RFC 2898)
  - bcrypt, scrypt
- Iteratívny výpočet - ZF(H,pw,n+1) = ZF(H,H(pw),n)
  - počet kôl ako parameter
  - časom zvyšovať zložitosť
  - dá sa meniť priebežne

4) Tajný kľúč

- Vylúčenie offline útokov
- Použitie
  - bloková šifra, napr. AES
  - špeciálny hash, napr. HMAC
- Pozor na uloženie kľúča
  - HSM, iba v pamäti...
- Stále treba soliť

Uloženie hesiel

- Vopred zvoliť:
  - zosilnenú funkciu, hash funkciu, počet iterácií, kľúč
- V DB:
  - user, salt, #iter
  - PBKDF2(HMAC(SHA256, key), pwd, salt, #iter)
- Priebežne:
  - zvyšovať iterácie
  - sledovať bezpečnosť hash funkcie

Dodatočná autentifikácia

- Čo ak bola ukradnutá identita?
- Ako zjednodušiť používateľovi bezpečnosť?

⇨ Citlivé operácie

- Pred vykonaním: dodatočná autentifikácia
  - znova primárna (napr. zadanie hesla),
  - alebo nový, špecifický postup

Najčastejšie metódy

- Špecifický mechanizmus dodatočnej auth:
  - ako rozložená viacfaktorová autentifikácia
  - bezpečnosť aspoň ako primárna autentifikácia
  - odporúčam silné metódy – nízke náklady, dostupnosť
- Obvykle:
  - kontrolný e-mail,
  - SMS,
  - sekundárne heslo,
  - bezpečnostná otázka/odpoveď.

e-mail, SMS

- Ide o prenesenie zodpovednosti
- web-mail
  - nízka miera opatrnosti používateľov
  - masovo realizované kompromitácie
- SMS
  - operátori negarantujú bezpečnosť
  - presmerovanie čísla, kompromitácia smartfónu

⇨Iba limitovaná bezpečnosť, nepoužívať samostatne.

Citlivé operácie

- Zmena bezpečnostných nastavení
  - parametre pre autentifikáciu (tel. číslo, e-mail)
  - ináč sa stráca zmysel dodatočnej auth.
- Zmena hesla
  - zadanie starého hesla a dodatočná auth.
  - rovnako odblokovanie konta
    - po prekročení neúspešných pokusov o prihlásenie

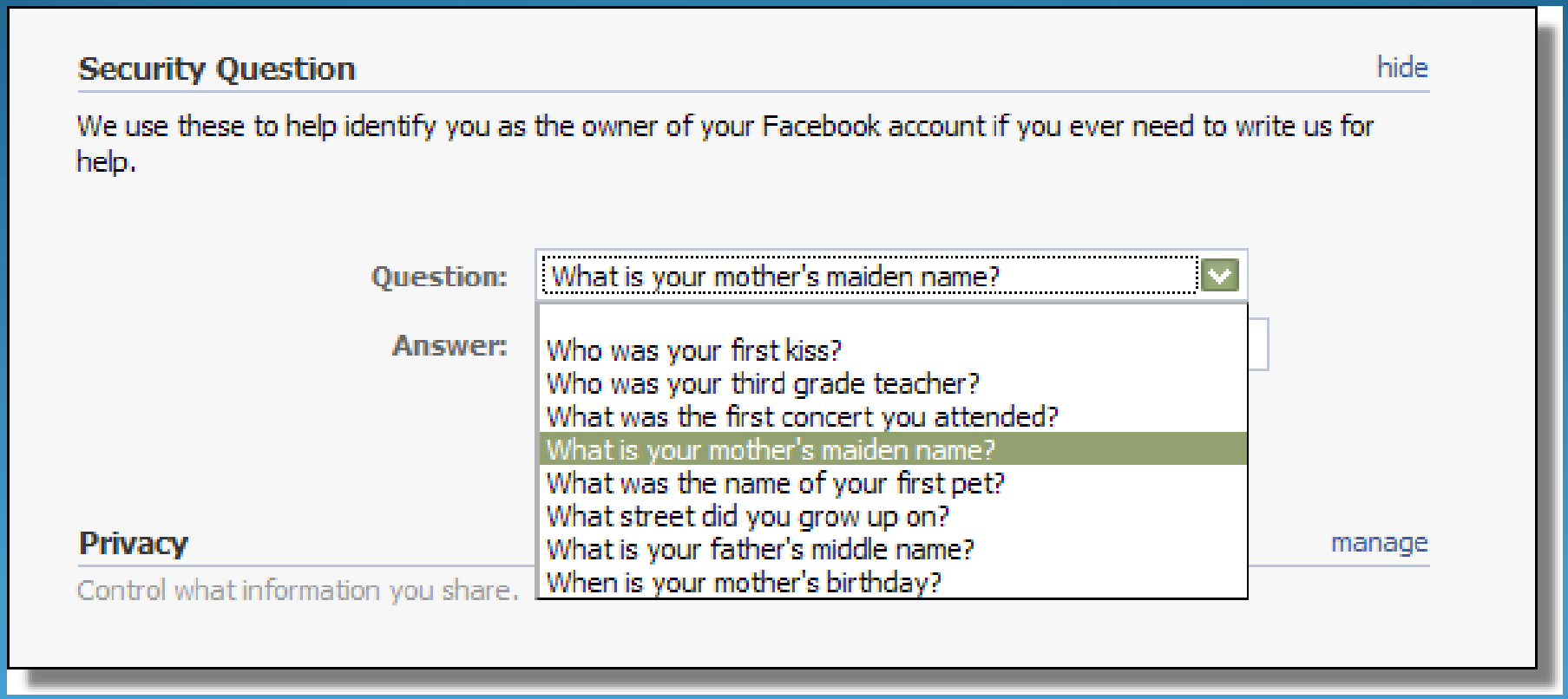
Citlivé operácie

- „Podozrivá situácia“
  - prihlásenie z neštandardnej lokality
  - neobvyklá operácia, parametre, vysoký počet operácií
  - aj každá rola samostatný okruh

  ⇨pozitívna spätná väzba o bezpečnosti

- Zabudnuté heslo
  - nestačí e-mail, SMS
  - odporúčam sekundárne heslo

Bezpečnostná otázka/odpoveď



Zdroj: www.f-secure.com

Dobrá otázka?

- Obľúbená farba?
- Meno domáceho zvieratka?
- Zmysel života, vesmíru a vôbec?
- Meno matky za slobodna?
- Dátum svadby?
- Číslo zdravotného poistenia?
- Miesto vlanajšej dovolenky?
- Prečo ma nikto nemá rád?

Dobrá otázka!

- bezpečná
  - veľký počet odpovedí, nie pravdepodobné odpovede
  - odpoveď nezistiť pozorovaním, prieskumom
  - ⇨ minimálne ako primárna autentifikácia/heslo
- nemenná
  - stále rovnaká odpoveď
- určitá
  - aby mi pomohla rozpamätať sa

Dĺžka odpovede

Znaková sada:	a-z, A-Z, 0-9, špec.znaky	a-z	text (ekvivalentné ~4 znaky na pozíciu)
Ekviv. dĺžka hesla:	6	8	19
	8	11	25
	10	14	32
	12	16	38
	14	19	44

Ďalšie komplikácie

- Bezpečné uloženie
  - odpoveď – ochrana ako pre heslo...
  - otázka – v otvorenom tvare
- Používateľ si „skoro“ pamätá
  - uzáme to?dĺžka
  - dá sa to zistiť?

~~Bezpečnostná otázka/odpoveď~~

- Radšej sekundárne heslo
  - menej záludností pri implementácii
  - lepšie povedomie o ochrane

Ďalšie oblasti

- timing attack
- heslová politika
- informovať používateľa
- testovanie hesiel
- blokovanie konta

- Ďakujem za pozornosť